536,818

(54) Title: MULTIPLIER WITH LOOK UP TABLES.
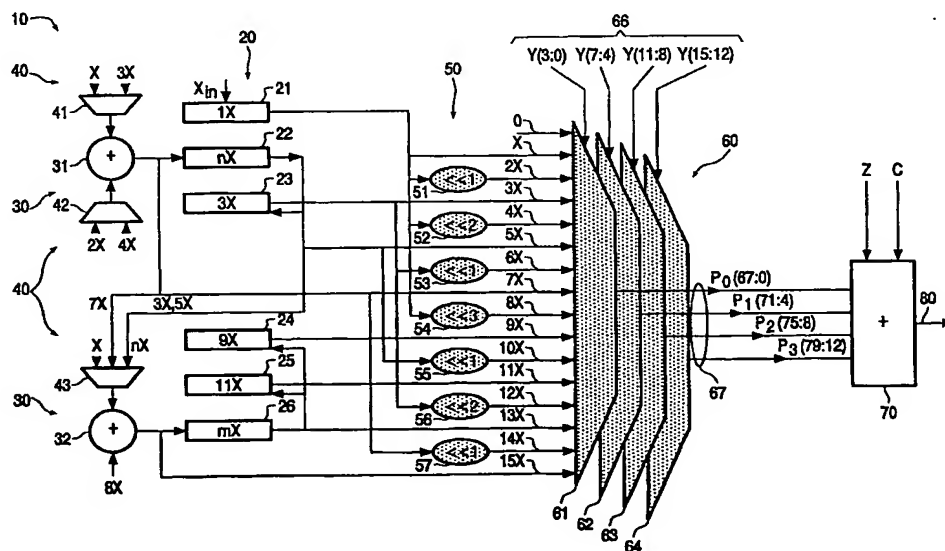
(57) Abstract: A method of performing modular multiplication of integers X and Y to produce a result R, where R = X.Y mod N, in
a multiplication engine. X is fragmented into a first plurality of words xn each having a first predetermined number of bits, k and Y
is fragmented into a second plurality of words yₙ each having a second predetermined number of bits, m. Multiples of a word xₙ of
X are derived in a pre-calculation circuit and subsequently used to derive products of the word xₙ of X with each of the plurality of
words yₙ of Y. An intermediate result Rⱼ is calculated as a cumulating sum derived from said pre-calculated multiples and the steps
repeated for each successive word of X so as to generate successive intermediate results, Rⱼ, for each of the first plurality of words
xₙ. The final result, R is obtained from the last of the intermediate results Rₙ₋₁.

WO 2004/051456 A2

*MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.